⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭61-264371

⑤1Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　昭和61年(1986)11月22日
G 09 C 1/00　7368-5B

審査請求　未請求　発明の数 2　(全7頁)

⑤4発明の名称　データ保護方式

⑳特　願　昭60-107134
㉒出　願　昭60(1985)5月20日

⑦2発明者　森　亮一　東京都文京区白山1-24-12
⑦1出願人　森　亮一　東京都文京区白山1-24-12
⑦4代理人　弁理士　長谷川　文廣　外1名

明　細　書

1．発明の名称

データ保護方式

2．特許請求の範囲

(1)　暗号化されたデータを，データ利用装置が解読して利用するシステムにおいて，

データを複数の暗号方式で複数通りに暗号化して供給し，この複数通りに暗号化されたデータのうちの1つまたはいくつかを解読する機能をもつ暗号解読手段と，

さらに上記供給されたデータのうちから上記1つまたはいくつかの，すなわち，暗号化されたデータ部分のうちから該暗号解読手段によって解読可能なものを識別する暗号方式識別手段とを該データ利用装置に設けたことを特徴とするデータ保護方式。

(2)　上記複数の暗号方式として，暗号アルゴリズムは同一であるが，複数の異なる暗号鍵を使用することを特徴とする特許請求の範囲第(1)項に記載のデータ保護方式。

(3)　上記データ利用装置内に設けた暗号解読手段を複数としたことを特徴とする特許請求の範囲第(1)項および(2)項に記載のデータ保護方式。

(4)　暗号化されたデータを，データ利用装置が解読して利用するシステムにおいて，

データを任意の暗号方式によって暗号化し，さらに該暗号化したデータを解読する手段を記述した情報を複数の暗号方式により複数通りに暗号化して上記暗号化したデータとともに供給し，この複数通りに暗号化された上記データ解読手段記述情報のうちの1つまたはいくつかを解読する機能をもつ暗号解読手段と，さらに上記複数通りに暗号化されている，データ解読手段記述情報のうちから，該暗号解読手段によって解読可能な情報部分を識別する暗号方式識別手段とを設けたことを特徴とするデータ保護方式。

(5)　上記複数の暗号方式として，暗号アルゴリズムは同一であるが，複数の異なる暗号鍵を使用す

ることを特徴とする特許請求の範囲第(4)項に記載のデータ保護方式。

(6) 上記データ利用装置内に設けた暗号解読手段を複数としたことを特徴とする特許請求の範囲第(4)項および第(5)項に記載のデータ保護方式。

3．発明の詳細な説明

〔概要〕

データを暗号化して流通させ，正当な利用者であると確認された利用者に対してのみ，該データの暗号を解読し，利用可能とするようなシステムに関して，暗号解読装置を製造する複数の製造者間，あるいは同一社内の複数グループ間で，暗号解読法の秘密を共有する危険を犯さずにすむための手段を提供する。

〔産業上の利用分野〕

本発明は，コンピュータ・プログラムやビデオ等のソフトウェアの保護，銀行の貯金残高等を含むデータなどの保護方式に関する。

〔発明の背景〕

近年，データ処理システムの発達と共に種々の有償プログラムが販売されるようになったが，その保護は不完全であり，プログラムの不正利用も多くなってきている。

またビデオテープや各種情報のデータについても同様な事情にある。

このように，同一のデータを多量に複製し，複数の装置によって利用させる場合，データの供給者が指定した装置でしか利用できないようにするのが，不正使用を防止するうえでの有効な手段となる。

このための基本的な方式は，第6図に示すように，データ利用装置①乃至⑤に対してデータaを提供する場合，データ利用装置ごとに異なる固有の鍵K_1乃至K_nでデータaを暗号化し，n個の暗号データ①乃至⑤を作成してそれぞれデータ利用装置に供給し，各データ利用装置では，対応する固有の解読鍵を用いて供給されたデータを排他的に解読するものである。

しかし，この方式では，暗号化されたデータを，データ本体の内容が同一であるにもかかわらず，データ利用装置の数と同じ数だけの種類用意しなければならないことから，大量複製，大量供給には不向きであった。

〔従来の技術〕

コンピュータ処理の分野では，提供したコンピュータ・プログラムを無断複製，無断使用から護るための手段として，公開鍵暗号方式を用いた方式が提案されている。この方式は，コンピュータの中に，解読鍵を封入した暗号解読装置を内蔵させ，この解読鍵に対応した暗号化鍵をプログラム製作者に対して公開し，プログラム製作者は，この暗号化鍵によって自己の製作したプログラムを暗号化して流通させる方式である。コンピュータ内部の暗号解読装置によってプログラムが解読されて実行されるが，解読された状態の生の形のプログラムがコンピュータ外部へ漏れることはない。

公開鍵暗号方式では，暗号化鍵が公開されていても，それに対応した解読鍵を推定することが事実上不可能であるため，暗号解読装置内部に封入された解読鍵が外部へ漏れない限り，製作者以外は，そのプログラムの内容を知ることができない。

従って，暗号解読鍵の秘密を守ることが，この方式を実施する場合に於いて重要となる。

【参考文献】

1.A.Lempel "Cryptology in Transition"
ACM Compyting Surveys,Vol.11,No.4,pp.285-304
2.M.E.ヘルマン，一松信訳「新しい暗号体系」
サイエンス，日本経済新聞社，
Vol.19,No.10,pp.100-112

〔発明が解決しようとする問題点〕

解読鍵の漏洩を防ぐ手段として，暗号解読装置を製造する製造装置によって自動的に解読鍵と暗号化鍵の対を生成し，暗号化鍵のみを生の形で外部に取り出し，解読鍵は，その装置から直接的に暗号解読装置内部へ書き込まれるようにし，生の

形の解読鍵が人間の目に触れることのないようにする方式が提案されているが，この方式による秘密保持は，製造装置がただ一つしか存在しない場合にのみ有効であり，複数の製造会社が暗号解読装置を製造する場合にはもちろん，ただ一社が製造する場合でも製造装置を複数台使用する場合には適用できない，という問題点を有していた。

〔問題点を解決するための手段〕

本発明は，上記の如き，解読鍵を秘密保持に関する問題点を克服することを目的としており，複数の会社が暗号解読装置を製造する場合には，各社が，又更に一社内では各製造装置毎に，それぞれ独立に自己の製造する装置に封入する鍵の秘密を守れば十分であるようにするものである。

この目的は，一つのデータの一部又は全部，あるいは暗号化されたデータの解読手段に関する情報の一部又は全部を，複数の暗号化鍵あるいは複数の暗号方式によって複数通りに暗号化し，暗号解読装置は，それらの暗号化部分から，自己の内部に封入されている解読鍵又は暗号解読手段に適合した部分を1つ選択し，そこのみを解読すれば，データを利用可能とすることによって達成される。

本発明の構成としては，暗号解読装置へ，暗号解読手段の他に，データの暗号部分のうち，どの部分が該暗号解読装置の持つ解読鍵又は暗号解読手段に適合した部分であるかを識別する手段を設けたことを特徴としている。

第1図は，本発明の原理的構成を示す図である。

図（A）は，データ本体を複数の暗号方式で複数通りに暗号化して，それぞれを暗号ブロックとし，それらを1つにまとめた並置暗号ブロックとして供給する方式の暗号データの構成を示している。図示の例では，データaがn通りに暗号化され，n個の暗号ブロックからなる並置暗号ブロックとして各データ利用装置に供給される。

図（B）は，データ本体をある1つの暗号方式で暗号化し，その解読鍵を複数の暗号方式で複数通りに暗号化したものをそれぞれ暗号ブロックとし，これらを暗号化したデータと一緒にまとめて供給する方式の暗号データの構成を示している。図示の例では，n通りに暗号化された解読鍵のn個の暗号ブロックからなる並置暗号ブロックと，暗号化されたデータaの単一の暗号ブロックとからなるデータとして各利用装置に供給される。

図（C）は，各データ利用装置内の構成を示し，1は暗号データ，2は暗号解読装置，3は暗号方式識別手段，4は暗号解読手段を表している。

暗号データ1は，図（A）あるいは図（B）に示されているような暗号データの構成をもつ。

暗号解読装置2は，本発明に基づく特徴的構成として，固有の暗号方式識別手段3および暗号解読手段4をそなえている。

暗号方式識別手段3は，暗号データ1の中の並置暗号ブロックの中から，自装置によって解読可能な暗号ブロックを識別し，取り出す。並置暗号ブロック中における暗号ブロックの位置は，予め配列内の順位で定められているか，インデックスで指定される。あるいは，順に全ての暗号ブロックの解読を試み，解読できたか否かで対応ブロックを識別してもよい。このとき暗号データ1の中の並置暗号ブロックから取り出される暗号ブロックは，図（A）の場合，暗号化されたデータaであり，図（B）の場合，暗号化された解読鍵である。

暗号解読手段4は，該手段に固有の解読鍵をこの取出された暗号ブロックに適用して解読する。このとき得られる解読結果は，図（A）の場合，データaであり，これで解読は完了する。図（B）の場合は暗号化されたデータaを解読するための解読鍵であり，暗号解読手段4は，これを用いてデータaを取出し，これで解読は完了する。

〔作用〕

ソフトウェアの例により，第2図の概念図にしたがって説明する。

ソフトウェアメーカは，ソフトウェア（□，△，○で表される）を開発すると，その少なくとも一部を第1図（A）あるいは（B）の形式で暗号化して出荷する。

ユーザは流通路から，暗号化された任意のソフトウェアを入手する。ユーザは，このソフトウェアを自由に複製することができ，ファイルシステムおよびネットワーク等の任意の場所へ蓄積することができる。また他人に譲渡することも自由である。

しかし，このソフトウェアは，暗号を解読しないかぎり実行し，利用することができない。利用可能なユーザのコンピュータには，第1図の暗号方式識別手段3および暗号解読手段4からなる暗号解読装置が備えられており，ここで解読できたソフトウェアのみが実行される。

〔実施例〕

第3図は，本発明の1実施例システムの説明図である。

図において，1は供給される暗号データ，1a1～1anは，同一のデータをそれぞれ異なった暗号方式によって暗号化した暗号ブロック，1bは1a1～1anの各暗号ブロックの先頭を指すインデックステーブル（INDEX），2i，2jは暗号解読装置であり，2iと2jは異なる製造会社によって製造されたものであってよい。3i，3jは，2i，2jそれぞれの内部に設けられた暗号方式識別手段，4i，4jは暗号解読手段である。

暗号解読装置2iへ暗号データ1を入力すると，暗号方式識別手段3iがインデックステーブル（INDEX）1bを読み取り，暗号解読装置2iへ設けられた暗号解読手段4iに対応した方式で暗号化された暗号ブロックが，1a1～1anのうちの何れであるか（この場合は1aiであるとする），および，その先頭の場所がどこであるかを決定し，暗号解読手段4iへ伝える。以後4iは，1a1の暗号を解読し，データを利用可能とする。暗号データ1が暗号解読装置2jへ入力された場合は，同様に，暗号データ1の中から1ajが選択され，暗号解読手段4jによって解読される。

暗号データ1a1～1an各々の大きさを一定不変としておけば，インデックステーブル（INDEX）1bを省略することができる。また，各暗号データ1a1～1anの先頭部を他の部分から識別可能な特殊なパターンとすることにより，あるいは，さらにそこへ暗号ブロックの識別情報を書き込むことにより，インデックステーブル（INDEX）1bを省略することもできる。

さらに全暗号ブロックについて総あたり的に解読を試み，正しく解読できたブロックを選択する方式もありうる。尚暗号データと暗号解読手段との組合わせによっては，解読できない場合もあり得ることは当然である。

本発明によれば，データ1a1～1anは，それぞれ別な暗号方式によって暗号化されており，それらは独立な暗号解読手段によって解読されるため，暗号解読装置を複数の会社が製造する場合，各製造者間で解読方式に関する秘密を共有する必要が無くなる。

このため，解読方式の秘密が漏洩する危険が減少するだけでなく，もし漏洩し，その暗号方式の使用を中止することになった場合，全ての解読装置を交換する必要がないため損害を最小限にくい止めることができる。

データを暗号化する複数の方式に何を選ぶかはデータ供給者の任意であるため，その選択によって，データ供給者はそのデータを利用することのできる暗号解読装置を指定することができる。このため，もし，暗号の秘密の保護が不完全である等，データ供給者にとって好ましくない会社の生産した暗号解読装置ではデータが利用できないようにすることが可能である。このことにより，暗号解読装置の生産者は，より完全な保護を提供しようと努めるようになる。

暗号方式として，暗号化するための鍵と，解読するための鍵が異なっており，暗号化するための鍵から解読するための鍵を推定することが事実上不可能である公開鍵暗号方式を用い，解読鍵と暗号化鍵のペアを暗号解読装置の製造者が作成し，解読鍵は暗号解読装置に封入して秘密とし，暗号化鍵のみをデータ供給者へ渡すことにすれば，解

読鍵の秘密保持が一層容易で，強力になる。

第4図は，本発明の他の実施例システムの説明図である。

図中，第3図と同記号のものは同じものを示している。第4図に特有の記号1aは暗号化されたデータ本体，1b'は暗号ブロック1d1～1dnの先頭を指すインデックステーブル（INDEX），1cはデータ1aを解読する手段を記述した情報，1d1～1dnは，それぞれ異なった方式で1cを暗号化した暗号ブロック，51は，暗号ブロック1diを解読するための第1暗号解読手段，61はデータ本体の暗号を解読するための第2暗号解読手段である。

次に，第5図の処理フローにしたがって動作を説明する。

データ1が暗号解読装置21へ入力されると，暗号方式識別手段31がインデックステーブル（INDEX）1b'を読み取り，その結果，暗号解読手段5iによって解読可能な暗号ブロックが1d1～1dnの中の何れであるかを識別する。これが1diであったとすると，次に暗号ブロック1diを第1暗号解読手段51へ読み込んで解読し，データ本体の解読手段記述情報1cを取り出して第2暗号解読手段61へ入力する。次に，データ本体1aを第2暗号解読手段61へ読み込み，61は，解読手段記述情報1cに基づいてデータ本体1aの解読を行う。

暗号を2段階にすることにより，1段階目，即ち，データ本体の暗号解読手段を記述したデータを暗号化した暗号ブロックについては，安全性は高いが，解読に時間がかかるために大量のデータを暗号化するには適さない暗号方式を適用し，安全性を高めることができる。

データ本体の暗号化には，解読速度の高い暗号方式を適用するが，この暗号方式の安全性がそれほど高くなかったとしても，この暗号方式は，各データ毎に異なるものとすることが可能であり，漏洩したときの損害は1段階目の暗号方式が漏洩した場合に比べ，少ない。

データの一部に，特に強力な保護を必要とする部分が有る場合，この部分は，他のデータと一緒に1aへ記録せず，データ本体の暗号解読手段を記述したデータと一緒に1d1～1dnへ記録する方式を採れば更に安全性を高めることができる。

なお，第3図の実施例において，暗号方式識別手段31が自装置に該当する暗号ブロック1a1を暗号データ1から取り出すために必要な内部情報，および取り出した暗号ブロック1a1を，暗号解読手段41が解読するために必要な解読鍵は，予め暗号解読装置内部のIC等に，ハードウェア的に封入しておけばよい。第4図の実施例における暗号方式識別手段3iおよび第1暗号解読手段5iについても同様である。

また，暗号方式識別手段あるいは暗号解読手段の処理ルーチンを暗号解読装置内部のIC等に封入することにより，通常のプログラムに全く意識させることなく，ソフトウェアの使用権確認，およびソフトウェアの暗号解読，を行わせることが可能である。しかし，これらの処理ルーチンをOSの一部として組み込み，解読鍵等はCPU IC等に封入しておいて，OSによってのみ参照可能にしてもよい。

〔発明の効果〕

以上述べた様に，本発明によれば，暗号解読装置を製造するメーカーは，その中に封入する暗号解読鍵の秘密は，自社内部，あるいは各製造装置毎に保護すればよく，他の，同一規格の暗号解読装置を製造するメーカーとの間で解読鍵の秘密を共有する必要や，鍵を，同一の鍵を使用する複数装置へ配るために装置外部へ露出させる必要が無くなる。

このことにより，秘密漏洩の危険が減少して，システム全体の信頼性が増す。又秘密保持に要するコストが減少でき，更に複数社が自由に暗号解読装置を製造できることになり，自由競争の原理が働く。

又，一つのデータについて複数の鍵による複数通りの暗号化を適用でき，内蔵した解読鍵の異なった複数種の暗号解読装置が存在できるため，仮

に一つの解読鍵が漏洩し，その鍵の使用を中止することになったとしても，そのためにリプレースする必要の有るのは，その解読鍵に対応した暗号解読装置のみであり，全ての暗号解読装置をリプレースする必要はなく，損害を最小限にくい止めることができる。

更にデータ供給者がそのデータを利用できる暗号解読装置を任意に指定することができるため，暗号解読装置製造者はより多くのデータ供給者から利用されるよう，暗号方式や，データ自体に関し，より完全な保護を提供するよう努力するようになる。

本発明は，有償のコンピュータ・プログラム，有償のビデオソフト，クレジットカード内の信用データ等，保護すべき全ての情報について適用可能である。

本発明の最大の効果は有体商品の取引においては当然であるところの品質向上や価格低下をもたらす自由競争と同様な競争を，データ保護における秘密保持の品質向上や価格低下に関して導入できることである。

4．図面の簡単な説明

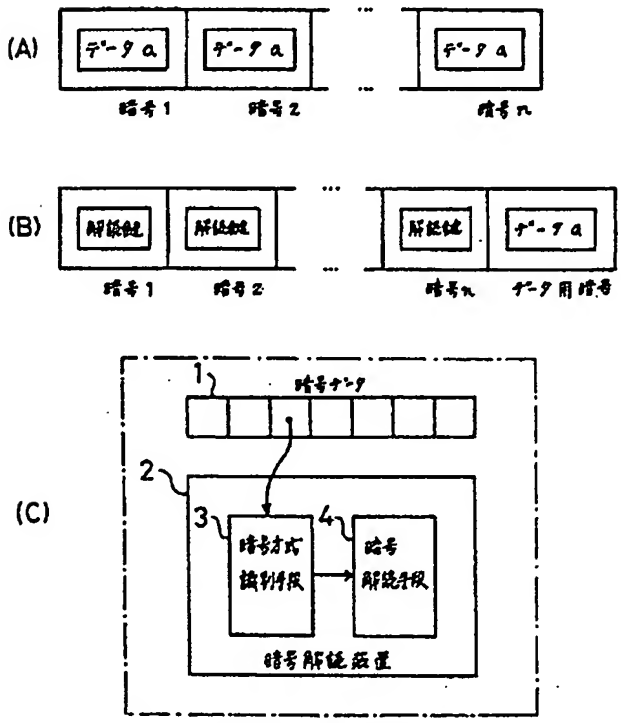
第1図は本発明の原理的構成を示す図，第2図は本発明の作用を説明する概念図，第3図および第4図はそれぞれ本発明の異なる実施例システムの説明図，第5図は第4図に示す実施例システムの処理フロー図，第6図は基本的なデータ保護の説明図である。

第1図において，

1は暗号データ，2は暗号解読装置，3は暗号方式識別手段，4は暗号解読手段を示す。

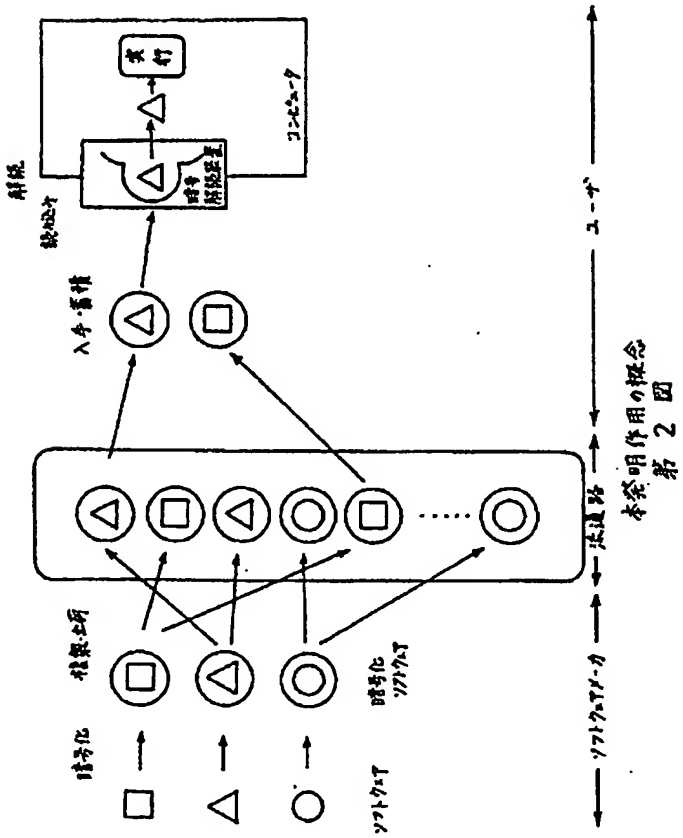
特許出願人　森　亮一

代理人弁理士　長谷川　文廣（外1名）



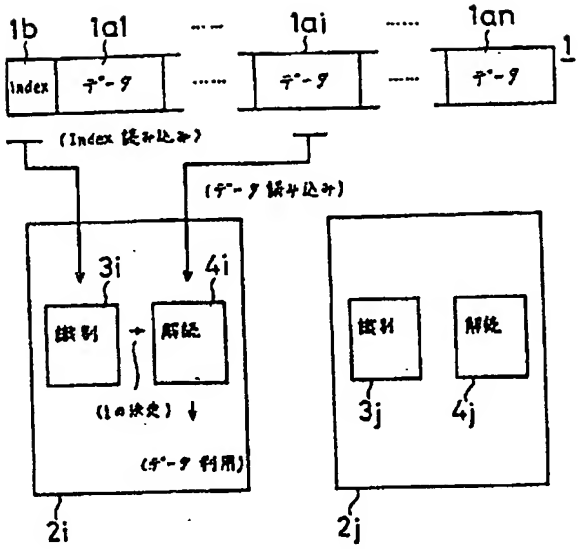
本発明の原理的構成

第1図



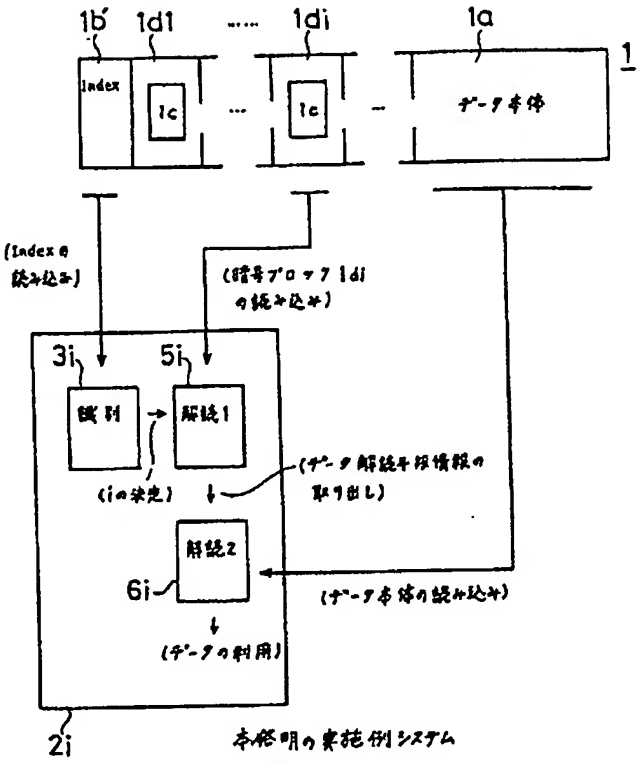
本発明作用の概念

第2図



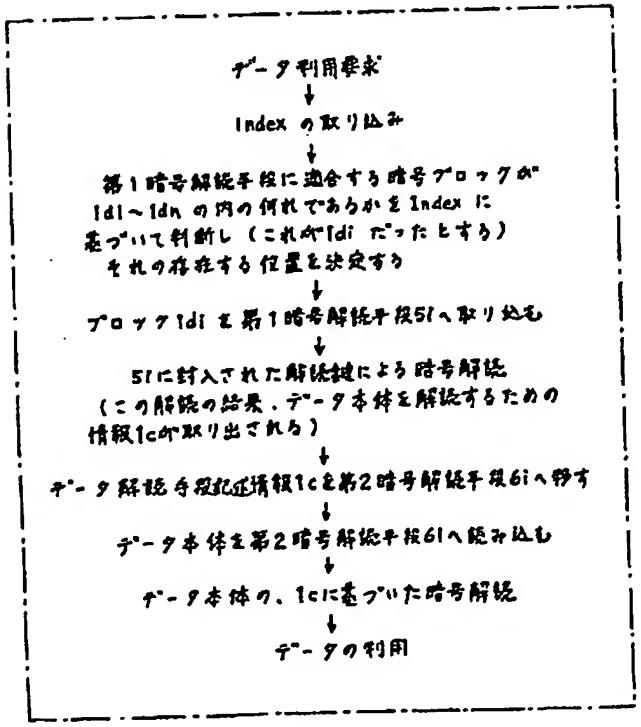
本発明の実施例システム

第 3 図



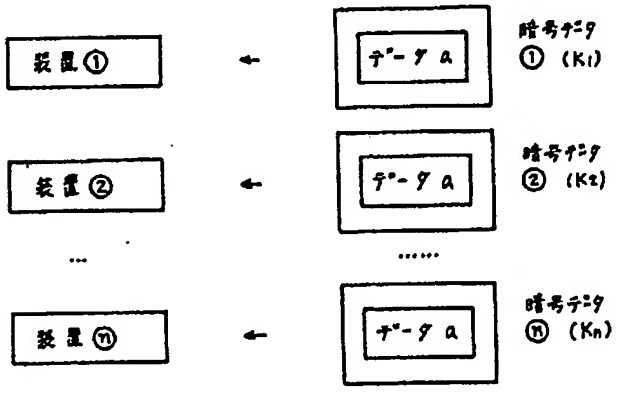
本発明の実施例システム

第 4 図



実施例の処理フロー

第 5 図



基本的なデータ保護の説明

第 6 図

(Translation)

The descriptions of Page 3 left top column Line 16 - right top column Line 3:

The purpose of the present invention would be achieve by means as follows:
1. A part or the whole of data, or a part or the whole of information regarding decode means for an encrypted data would be encrypted in plural way by plural encryption keys or plural encryption methods.
2. A decoder will select one unit among these encrypted data or information that would be appropriate for the decryption key or the decoder thereof.
3. It would be possible to use the encrypted data just by decoding the part of them.

[And Fig.1 shows the basic idea of the description above. We also attached herewith a translation of Fig.1]

The descriptions of Page 3 bottom top Line 15 - Page 4 right top Line 19:

After developing software (which are represented by marks "□", "△", or "○" in the Figure), software benders provide their products in which at least a part of software has been encrypted in the way of Fig.1 (A) or Fig.1 (B).

Users obtain encrypted software from a distribution channel. A user can copy the software freely, and he can store the software on a certain place of a file system or a network.

However, the software is not available, nor executable unless decryption. Permitted user's computers have decoders comprising Cipher System Description Means 3 and Decryption Means 4. Only software that has been decrypted by the decoder would be executed.

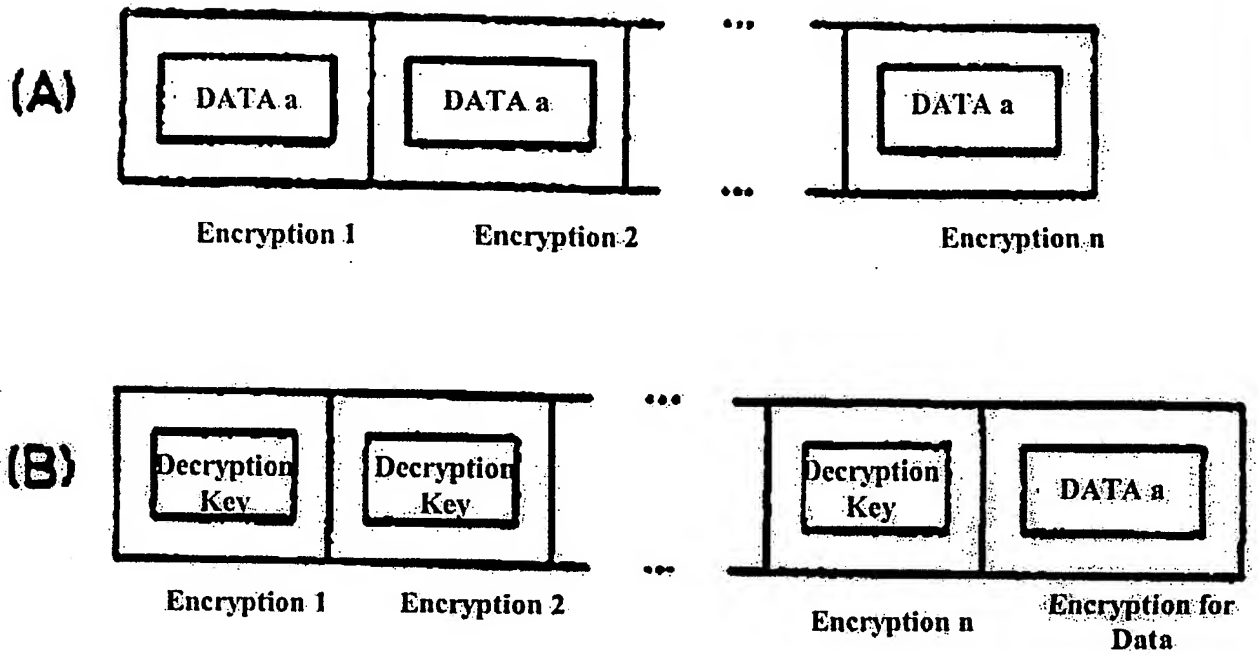
[Embodiment]

Figure 3 shows an embodiment of the system according to the present invention. In the Figure 3, "1" is an encrypted data provided to the system, 1a1-1an are encrypted blocks encrypted by different encryption methods respectively. 1b is an index table (INDEX) that points each head address of the encrypted blocks. 2i and 2j are decoders, which may be produced by different companies. 3i and 3j are Cipher System Description Means, which are inside of 2i and 2j respectively. 4i and 4j are Decryption Means.

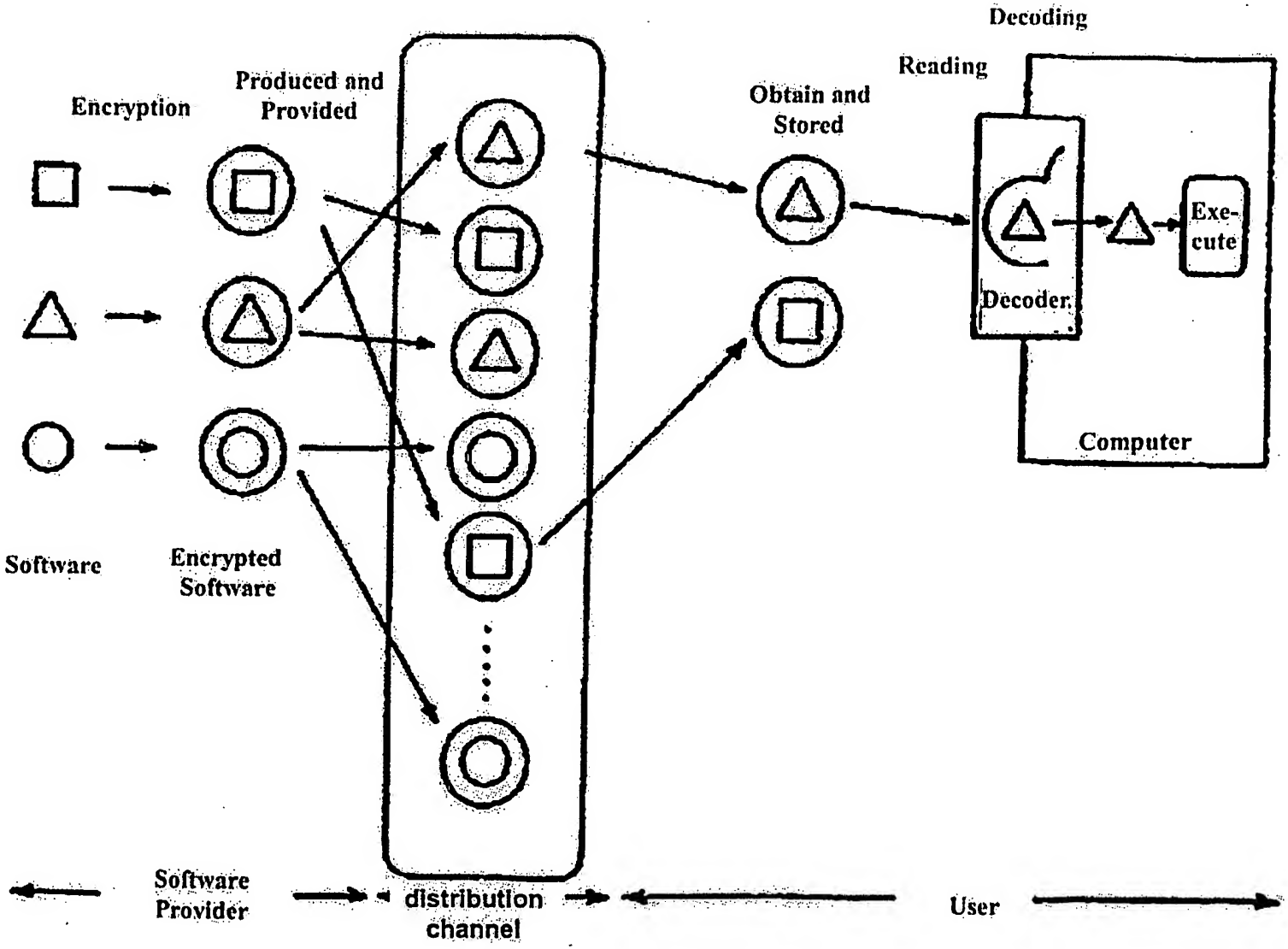
When encrypted data 1 is entered in decoder 2i, Cipher System Identification

Means 3i reads the index table (INDEX) 1b and determines two matters; 1) among 1a1-1an, which is the encrypted block corresponding to Decryption Means 4i for the decoder 2i, and 2) where is the head address thereof, and sends the information to Decryption Means 4i. Since then, 4i decodes the encrypted data of 1ai and the data would be available.

When encrypted data 1 is entered in decoder 2j, similarly, 1aj is selected among encrypted data 1 and that would be decoded by Decryption Means 4j.

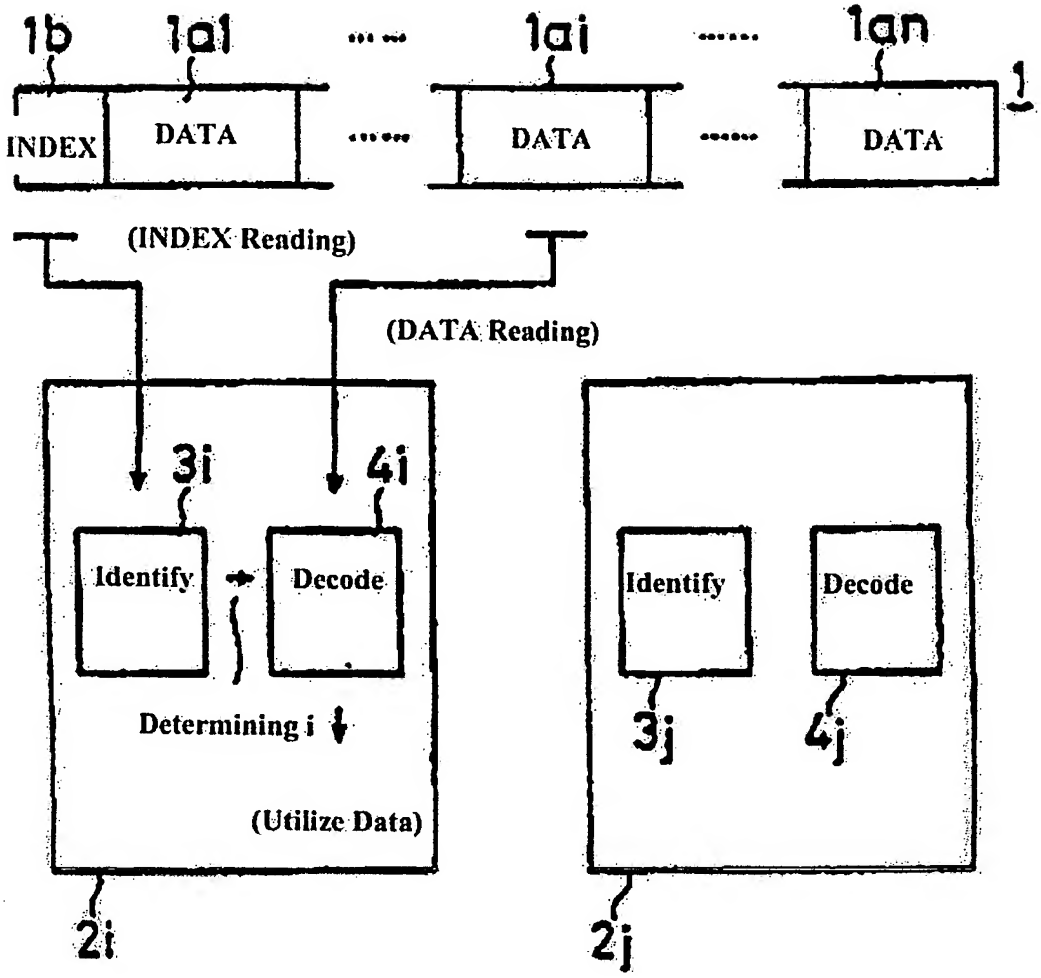


The basic composition of
the present invention
Fig. 1

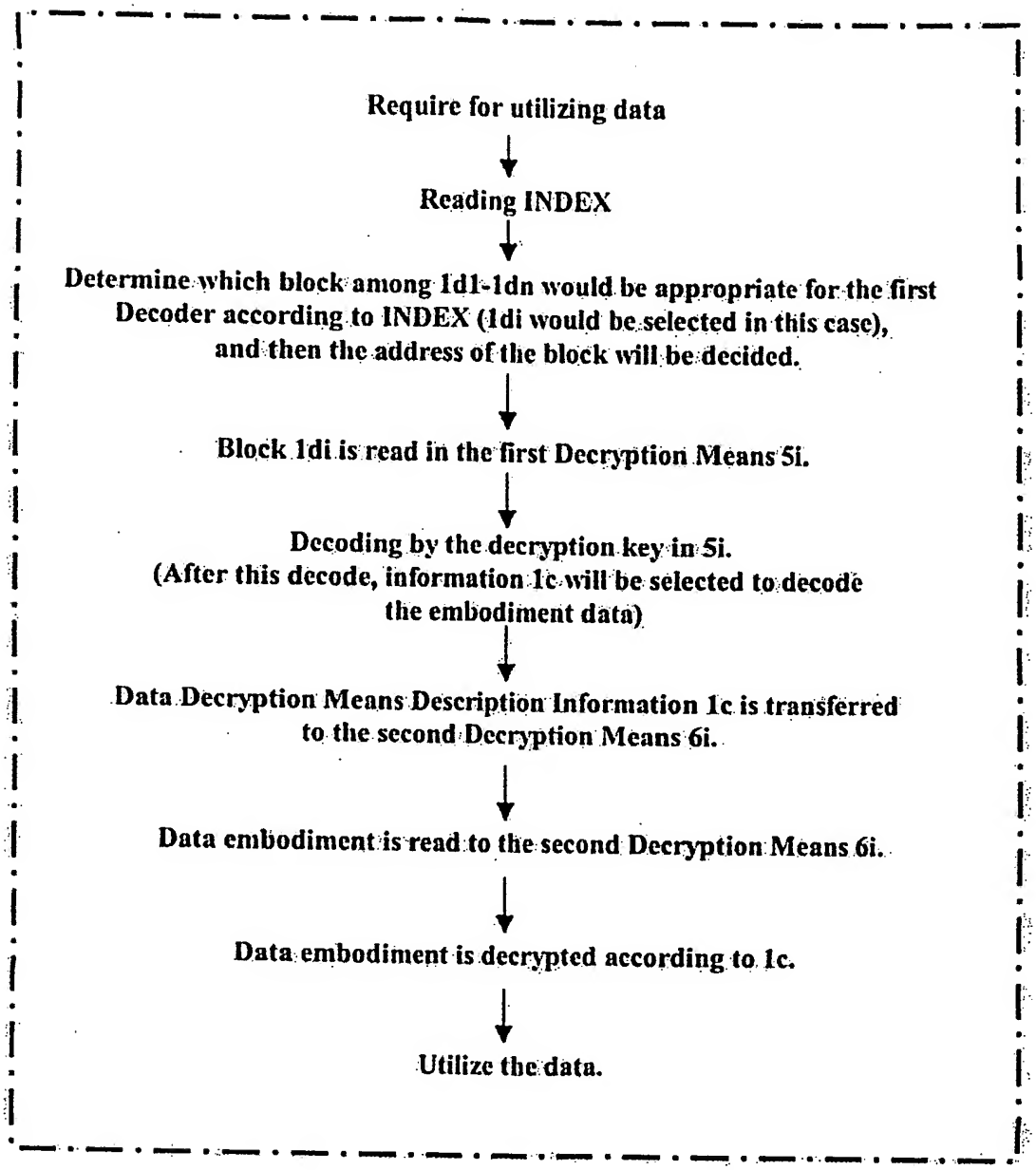


Concept of the present invention

Fig. 2



Embodiment system of the
present invention
Fig. 3



Flow chart of the embodiment
Fig. 5